## ARTIFACT SHEET

Enter a	rtifact number below. Artifact number is application number + type code (see list below) + sequential letter (A, B, C). The first
artifact	folder for an artifact type receives the letter A, the second B, etc
	les: 59123456PA, 59123456PB, 59123456ZA, 59123456ZB
Exampl	les: 59123450PA, 59125450PB, 59125450ZA, 59125450ZB
· - •	
Indicate	e quantity of a single type of artifact received but not scanned. Create
individ	ual artifact folder/box and artifact number for each Artifact Type.
	CD(s) containing:
L	computer program listing  Doc Code: Computer  Artifact Type Code: P
	pages of specification
	and/or sequence listing
	and/or table  Doc Code: Artifact  Artifact Type Code: S
	content unspecified or combined
	Doc Code: Artifact Artifact Type Code: U
	Doc Code. Addition
	Stapled Set(s) Color Documents or B/W Photographs
	Doc Code: Artifact   Artifact Type Code: C
	Microfilm(s)
	Doc Code: Artifact Type Code: F
	Video tape(s)
	Doc Code: Artifact Type Code: V
	Model(s)
	Doc Code: Artifact Artifact Type Code: M
	D 1 D
	Bound Document(s)  Doc Code: Artifact
L	Doc Code. Artifact Type Code. B
	Confidential Information Disclosure Statement or Other Documents
	marked Proprietary, Trade Secrets, Subject to Protective Order,
	Material Submitted under MPEP 724.02, etc.
	Doc Code: Artifact Artifact Type Code X
	· ·
	Other, description:
	Doc Code: Artifact Artifact Type Code: Z



# The United States of America



## The Commissioner of Patents and Trademarks

Has received an application for a patent for a new and useful invention. The title and description of the invention are enclosed. The requirements of law have been complied with, and it has been determined that a patent on the invention shall be granted under the law.

Therefore, this

## United States-Patent

Grants to the person(s) having title to this patent the right to exclude others from making, using, offering for sale, or selling the invention throughout the United States of America or importing the invention into the United States of America for the term set forth below, subject to the payment of maintenance fees as provided by law.

If this application was filed prior to June 8, 1995, the term of this patent is the longer of seventeen years from the date of grant of this patent or twenty years from the earliest effective U.S. filing date of the application, subject to any statutory extension.

If this application was filed on or after June 8, 1995, the term of this patent is twenty years from the earliest effective U.S. filing date of the application, subject to any statutory extension.

Buce Tehman

Commissioner of Patents and Trademarks

Michiller Haller



### US005548646A

## United States Patent [19]

Aziz et al.

[11] Patent Number: 5,548,646

**Date of Patent:** [45]

Aug. 20, 1996

[54] SYSTEM FOR SIGNATURELESS TRANSMISSION AND RECEPTION OF DATA PACKETS BETWEEN COMPUTER **NETWORKS** 

[75] Inventors: Ashar Aziz; Geoffrey Mulligan, both

of Fremont, Calif.; Martin Patterson, Grenoble, France; Glenn Scott,

Sunnyvale, Calif.

[73] Assignee: Sun Microsystems, Inc., Mountain

View, Calif.

Appl. No.: 306,337 [21]

[22] Filed: Sep. 15, 1994

Int. Cl.<sup>6</sup> ...... H04K 1/00 [51]

[56]

#### References Cited

#### U.S. PATENT DOCUMENTS

5,204,961 4/1993 Barlow ...... 380/25 5,416,842 5/1995 Aziz ...... 380/4

Primary Examiner-David C. Cain Attorney, Agent, or Firm-Matthew C. Rainey

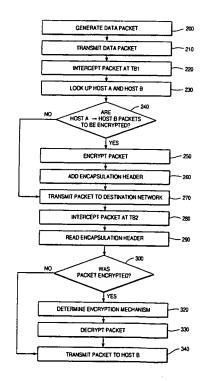
[57]

## **ABSTRACT**

A system for automatically encrypting and decrypting data packet sent from a source host to a destination host across a public internetwork. A tunnelling bridge is positioned at each network, and intercepts all packets transmitted to or from its associated network. The tunnelling bridge includes

tables indicated pairs of hosts or pairs of networks between which packets should be encrypted. When a packet is transmitted from a first host, the tunnelling bridge of that host's network intercepts the packet, and determines from its header information whether packets from that host that are directed to the specified destination host should be encrypted; or, alternatively, whether packets from the source host's network that are directed to the destination host's network should be encrypted. If so, the packet is encrypted, and transmitted to the destination network along with an encapsulation header indicating source and destination information: either source and destination host addresses, or the broadcast addresses of the source and destination networks (in the latter case, concealing by encryption the hosts' respective addresses). An identifier of the source network's tunnelling bridge may also be included in the encapsulation header. At the destination network, the associated tunnelling bridge intercepts the packet, inspects the encapsulation header, from an internal table determines whether the packet was encrypted, and from either the source (host or network) address or the tunnelling bridge identifier determines whether and how the packet was encrypted. If the packet was encrypted, it is now decrypted using a key stored in the destination tunnelling bridge's memory, and is sent on to the destination host. The tunnelling bridge identifier is used particularly in an embodiment where a given network has more than one tunnélling bridge, and hence multiple possible encryption/decryption schemes and keys. In an alternative embodiment, the automatic encryption and decryption may be carried out by the source and destination hosts themselves, without the use of additional tunnelling bridges, in which case the encapsulation header includes the source and destination host addresses.

#### 17 Claims, 7 Drawing Sheets



six on the the the of